SERVICIOS NATIVOS

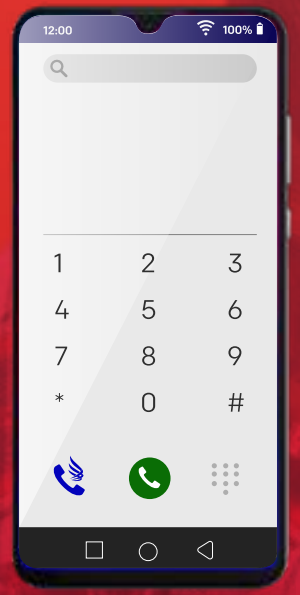
Maximiza todas las funciones incorporadas en un solo marcador

Hybrid Dialer™

GSM+VoIP

Primer marcador híbrido en el mundo, que integran tecnología GSM y VoIP como aplicación nativa.

No dependes de apps externas.



Distintas opciones de llamada en un solo marcador.

Configura llamadas GSM y VoIP en el mismo teclado.

Wings mobile

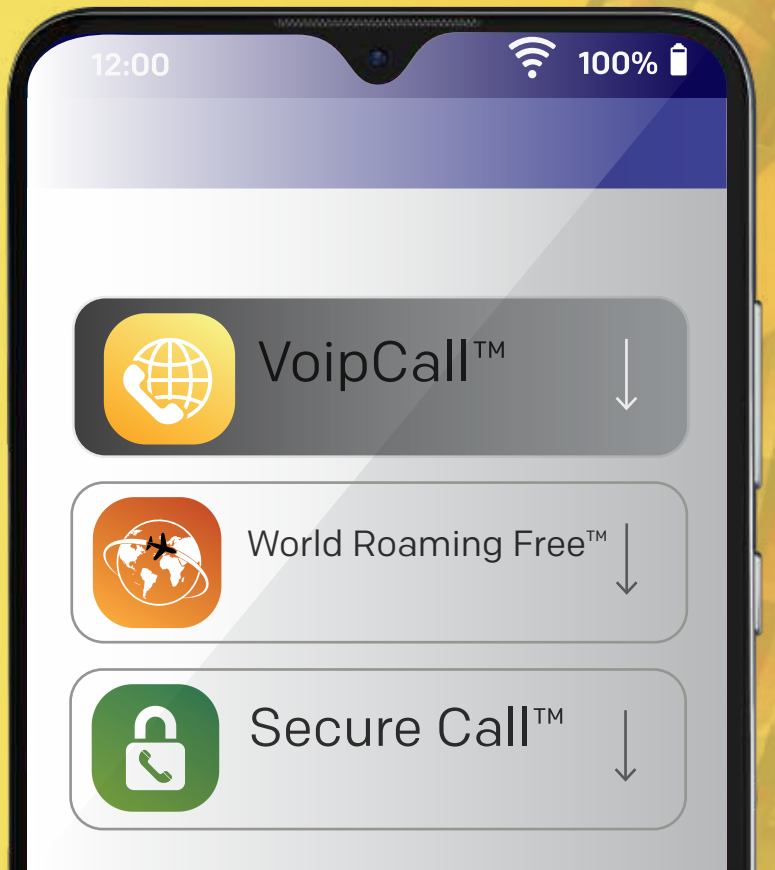
Guardian™

Es un **sistema de seguridad que verifica en tiempo real** si otras aplicaciones instaladas o troyanos, utilizan el micrófono o la cámara sin el conocimiento del usuario.

Protege la cámara de capturas
y el micrófono de audios sin tu consentimiento.

Wings mobile

VoipCall™



AHORRA UN 90%

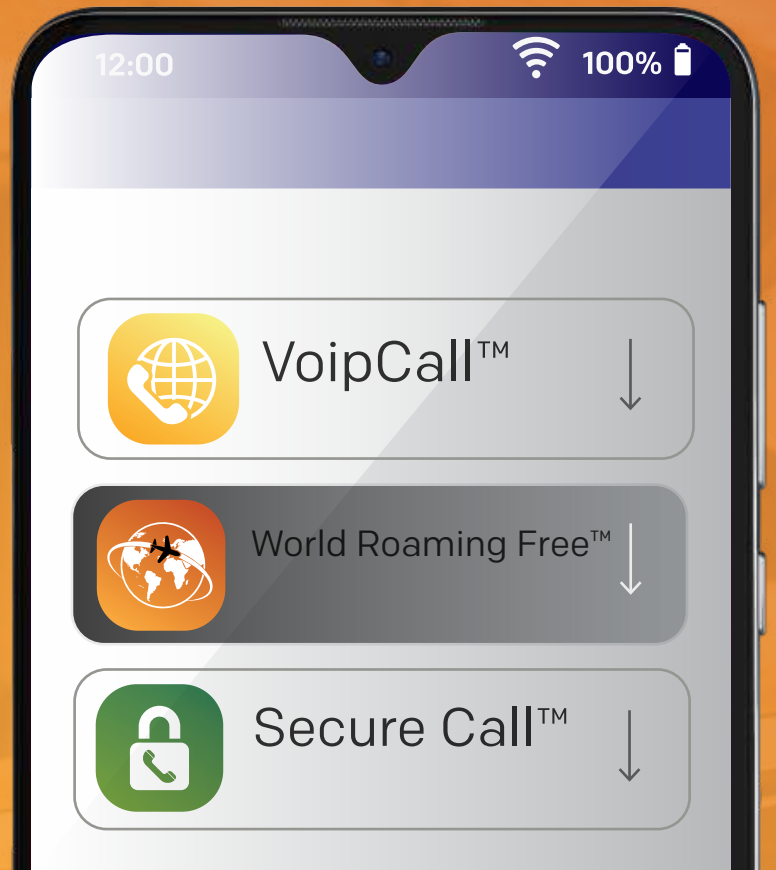
La posibilidad de usar **servicios exclusivos en llamadas VoIP**, con acceso a planes de tarifas especiales permitiendo ahorrar un 90% en comparación a otros mercados que no son sólidos.

Wings mobile

World Roaming Free™

Llama a todo operador

Disponible en 60 países

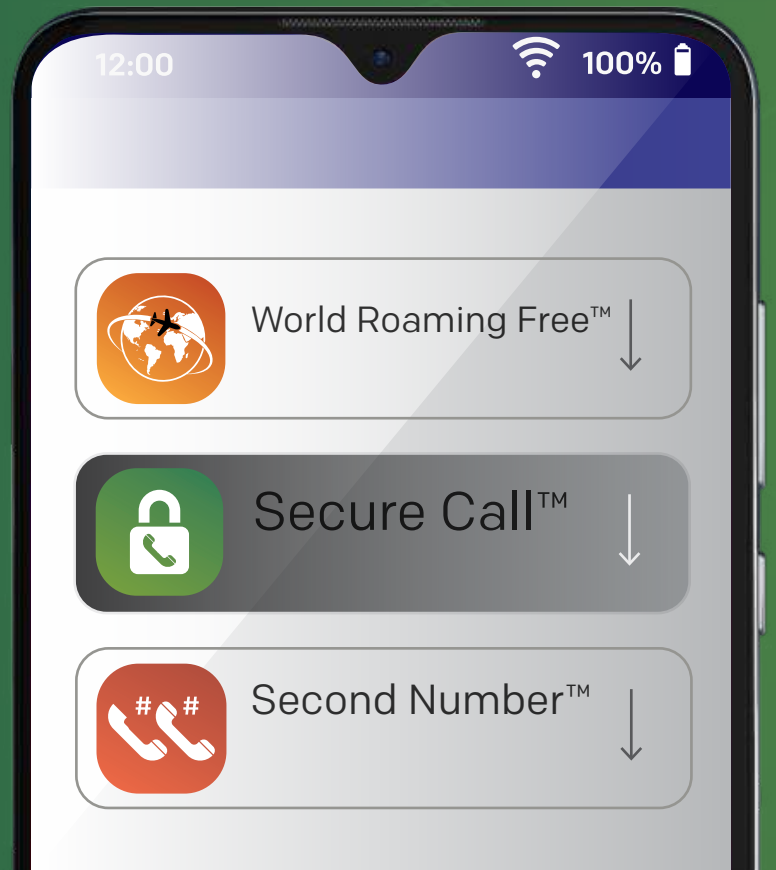


¡TOTALMENTE GRATUITO!

Único sistema en el mundo que **convierte las llamadas GSM entrantes en llamadas VoIP**, de forma totalmente gratuita en cualquier lugar donde exista una conexión a Internet.

Wings mobile

Secure Call™



TRIPLE NIVEL DE SEGURIDAD

Llamadas seguras y protegidas por un triple nivel de seguridad: DTLS (Transport Layer Security) para la comunicación por Internet, ZRTP (Zimmermann real-tiempo real de transporte Protocolo) para un intercambio de extremo a extremo protegido mediante claves de cifrado, y la tecnología ICE para P2P. Ningún flujo de datos VoIP pasa por el servidor, lo que garantiza que incluso Wings Mobile no pueda interceptar las llamadas.

ZRTP

ZRTP proporciona una encriptación de extremo a extremo para llamadas VoIP es decir, solo voz con IP.

DTLS

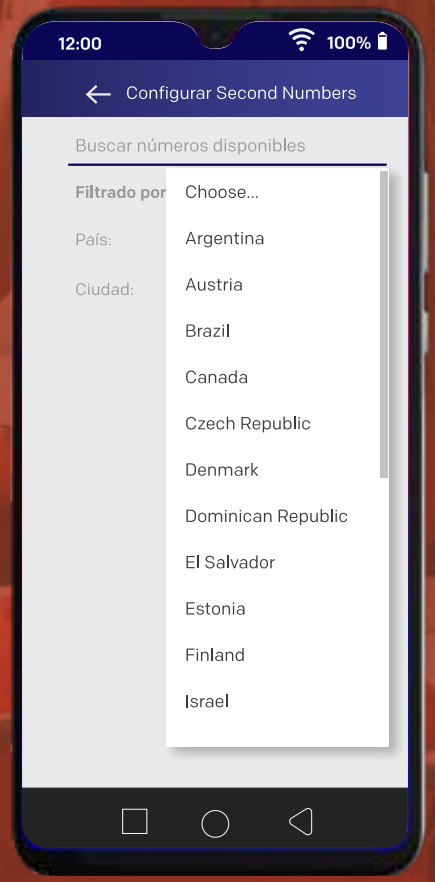
La Extensión de Seguridad de la Capa de Transporte de Datagramas (DTLS) establece claves para la seguridad en tiempo real. El Protocolo de Transporte (SRTP) al igual que el ZRTP, el SRTP-DTLS (RFC 5764), proporciona una encriptación de extremo a extremo, pero se basa en una clave pública/privada para encriptar los intercambios de claves.
Sus principales características son:
-Encriptación de extremo a extremo basada en la moderna criptografía de curva elíptica.
- Privacidad completa hacia adelante con un algoritmo de doble trinquete.
- Detección de “hombre en el medio” basada en la función auxiliar del ZRTP.t

Wings mobile

Second Number™

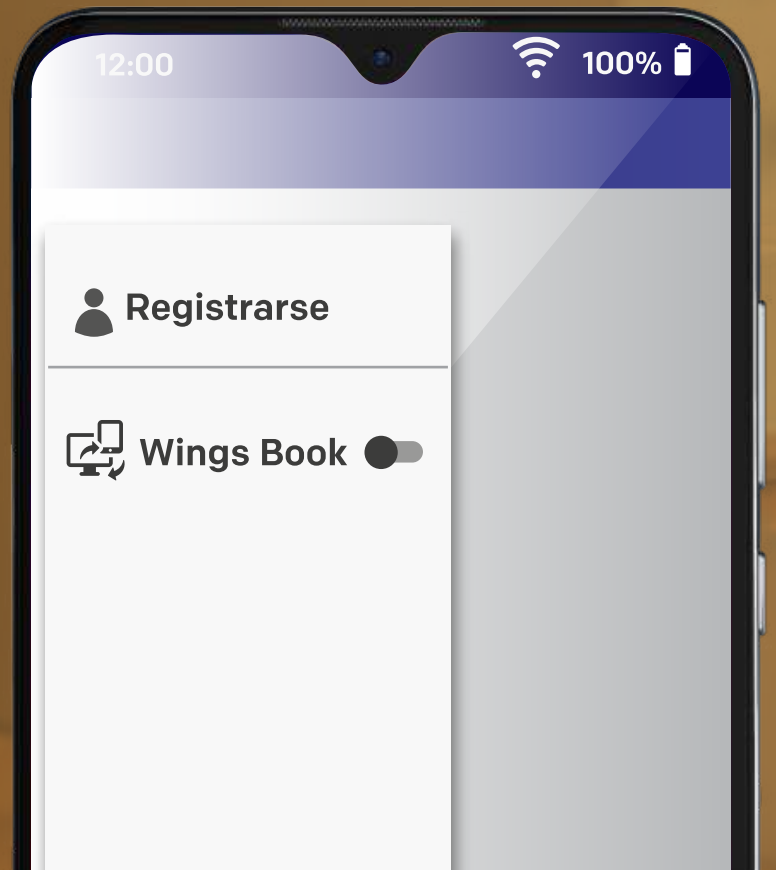
HAZ Y RECIBE LLAMADAS CON TU SEGUNDO NÚMERO

Servicio exclusivo, disponible en todos los teléfonos inteligentes de Wings. **Permite a los usuarios elegir los números de teléfono adicionales** que necesite.



Wings mobile

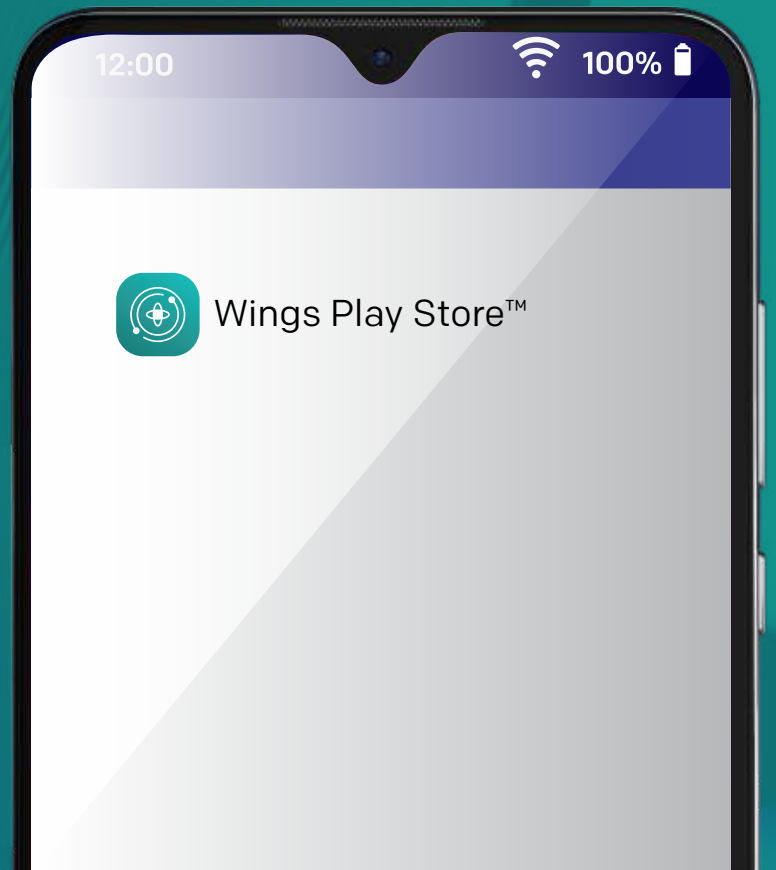
Wings Suite™



Permite a los usuarios **transferir todas las funciones de WINGS PHONE directamente en el portátil WINGS BOOK,** incluidas las llamadas GSM de cualquier operador de telefonía móvil.

Wings mobile

Wings Play Store™



Garantiza total privacidad de las App's instaladas y sus transacciones

Todos nuestros dispositivos Wings Phone TM, ofrecen una **plataforma de distribución para aplicaciones de Smartphone anónima** dirigida por WINGS MOBILE. No necesita registro por correo electrónico.

Wings mobile

ZRTP

Extensión Zimmermann Real-time Transport Protocol

Es un protocolo de intercambio en claves criptográficas destinado para asignar las claves de cifrado entre dos puntos finales en la telefonía de voz sobre un protocolo de internet llamado (VoIP).
En otras palabras, ZRTP proporciona llamadas encriptadas de extremo a extremo sobre una red VoIP, no efectiva en llamadas GSM u otros tipos de telefonía, solo llamadas de voz sobre IP.

Es muy importante tener presente esta última aclaración.

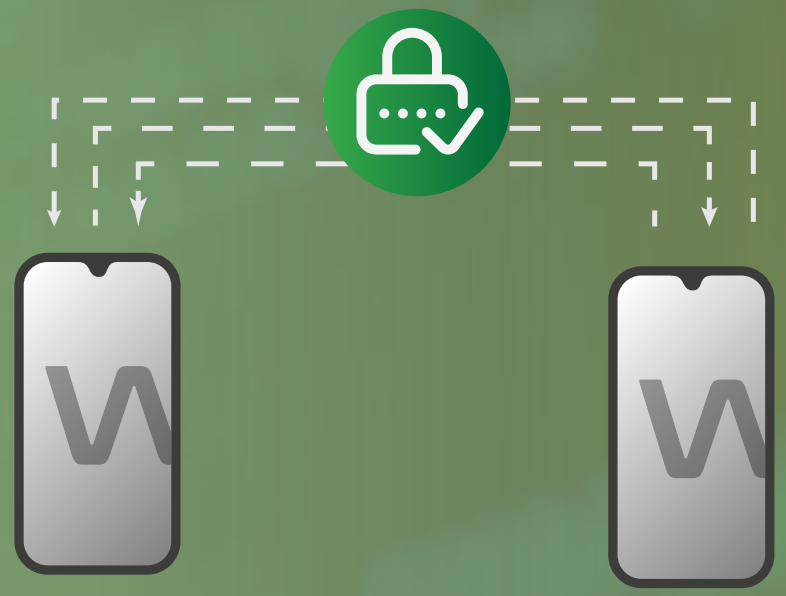
En la fase de descubrimiento de claves, el emisor y el receptor intercambian sus identificaciones ZRTP, así como información sobre las versiones de ZRTP compatibles, las funciones hash, los cifrados, las longitudes de las etiquetas de autorización y el acuerdo de clave de cada uno.

Tipos de algoritmos SAS.

Los mensajes intercambiados en la primera fase se llaman "Mensaje de saludo" o “Hello message”. Un reconocimiento llamado HelloACK message, se enviará al recibir un "Mensaje saludo".

Después de verificar la compatibilidad, el emisor elige cuál es la función de cálculo, cifrado, longitudes de las etiquetas de autorización, tipos de acuerdo en claves y algoritmos “SAS” que se deben usar, basando su elección en la información que es traída en los "Mensajes de saludo".

Estos datos se enviarán al receptor a través de un mensaje llamado “commit” o “confirmación”. El emisor necesita generar un par de claves rápidas antes de enviar la confirmación, y el receptor genera sus propias claves antes de enviar un mensaje llamado DHPart1.
Los valores públicos de Diffie-Hellman son intercambiados en los mensajes DHPart1 y DHPart2. ZRTP requiere generar nuevas claves Diffie-Helman para cada sesión.



LUEGO SE CALCULAN LAS CLAVES CRIPTOGRÁFICAS ZRTP Y LAS SALTS.

Finalmente, la fase de confirmación tiene lugar a través de los mensajes “Confirm 1” y “Confirm 2”.

Estos contienen el intervalo de caducidad en el caché para generar el más reciente código secreto. Extensión de Datagram Transport Layer Security (DTLS) para establecer claves en un protocolo seguro de tiempo real. (SRTP) Al igual que ZRTP, SRTP-DTLS (RF5764) proporcionan cifrado de extremo a extremo, pero se basa en una clave pública/privada para cifrar intercambios. Los certificados X509 se utilizan para la autenticación.

La principal ventaja de este protocolo es la inter-operabilidad con WebRTC. La implementación de Linphone de SRTP-DTLS se basa en la biblioteca mbedTLS, mejorada con un parche específico y mantenida por comunicaciones Belledonne.

Las características principales son:

- Cifrado de extremo a extremo basado en la criptografía moderna de curva elíptica
- Secreto directo perfecto con algoritmos de doble trinquete
- Detección de terceros en el medio basada en el auxiliar secreto ZRTP
- Protocolo de señalización agnóstico y estructura

Wings mobile

DEFENSA DE ATAQUES POR TERCEROS EN EL MEDIO

Aunque ZRTP utiliza un algoritmo de clave pública, no requiere infraestructura de claves (PKI).
No utiliza claves públicas constantes en absoluto. En cambio, el protocolo emplea un proceso rápido Diffie Hellman con vínculo hash y permite la detección de ataques por terceros en el medio de la comunicación (MiTM), al mostrar una cadena de autenticación corta (SAS) que los usuarios comparan por teléfono.

Es importante tener en cuenta que el proceso Diffie-Hellman ayuda con los intercambios de claves, usando siempre las claves privadas de DH. Por lo tanto, cada vez que los usuarios o terminales realizan un intercambio de claves DH, terminan compartiendo entre ellos información secreta sin ser intervenida por otros.

Con la fase Diffie-Hellman, se genera una clave DH temporal para cada conexión, por lo que ninguna clave se utiliza dos veces. Además, esto permite la comunicación secreta de manera directa, también conocido como “secreto directo perfecto”. significa que incluso, si una clave se filtra, la comunicación ya establecida sigue siendo segura debido a la protección por diferentes claves.

En algún momento si los usuarios no quieren tener cadenas de autenticación cortas, ZRTP ofrece una protección contra MiTM, debido a la continuidad de la clave. Lo hace almacenando en el caché algún código clave para usar en la próxima llamada y así entrelaza el secreto compartido DH de la siguiente llamada a realizar. Esto proporciona propiedades de continuidad en clave similar a las autorizaciones de certificados e identificación encriptada.

Wings mobile

Este proceso puede presentar alguna dificultad para entenderlo, pero en realidad no es difícil. Como se ha explicado, todo esto se hace sin depender de una PKI (infraestructura de clave pública), certificado de claves, modelos de confianza o gestión de claves continuas. De hecho, no se basa en el protocolo de iniciación de sesión (SIP) para la gestión de claves. No depende de ningún servidor en absoluto. Realiza sus acuerdos y gestión de claves directamente de punto a punto a través de la secuencia de paquetes RTP. También es compatible con el cifrado adaptable mediante una detección automática, si los otros usuarios de VoIP son compatibles con el proceso ZRTP.

Wings mobile

Exactamente, ¿cómo te protege Wings Phone y ZRTP, contra un ataque de terceros en el medio de la comunicación (MiTM)?

El intercambio de claves Diffie-Hellman, ZRTP utiliza una cadena de autenticación corta (SAS), que es esencialmente un hash criptográfico de los dos valores de Diffie-Hellman. El valor SAS se representa en ambos puntos finales de ZRTP, para llevar a cabo la autenticación. El valor SAS se lee en voz alta al interlocutor a través de la conexión de voz. Si los valores en ambos extremos no coinciden, indica la presencia del ataque por medio de un tercero en la comunicación. Si coinciden los valores, hay una alta probabilidad de que no haya ningún tercero escuchando.

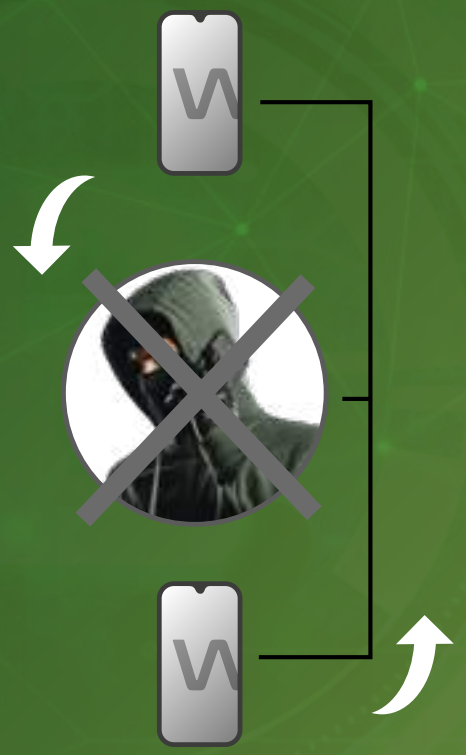
El uso del compromiso hash en el intercambio DH, limita al atacante a solo una suposición para generar el SAS correcto en el posible ataque, lo que representa que el SAS puede ser bastante corto.
Un SAS de 16 bits, por ejemplo, proporciona al atacante una sola oportunidad en vez de 65.536 para no ser detectado.

ZRTP proporciona un segundo escudo de autenticación contra un ataque MiTM, basada en una forma de continuidad en clave. Lo hace almacenando en el caché parte del material de clave compartido con hash para usarla en la próxima llamada, mezclando el secreto compartido DH de la siguiente llamada, dándole propiedades de continuidad de clave análogas a SSH. Si el MiTM no está presente en la primera llamada, queda la comunicación segura.

Wings mobile

Por lo tanto, incluso si el SAS nunca se usa, la mayoría de los ataques MiTM se detienen, porque no estuvieron presentes en la primera llamada. Las características de clave y continuidad ZRTP tienen algunas propiedades de restauración que son mejores que el enfoque SSH.

ZRTP proporciona un tercer escudo de protección contra un ataque MiTM. El IEDTF incorpora protección de integridad a la entrega de información SIP, y esa protección de integridad responderá en una PKI. Cuando esto finalmente se implemente, ZRTP puede aprovecharlo. Consulta cómo RFC 6189 y ZRTP puede aprovechar un escudo SIP protegido para proporcionar protección de integridad en el intercambio Diffie-Hellman de ZRTP.

Todo este proceso protege la comunicación contra un ataque MiTM, sin hacer que los usuarios comparen verbalmente el SAS. Sin embargo, todavía no hay un proceso VoIP que ofrezca la secuencia SIP completa y genere protección integrada de extremo a extremo para la entrega de información SIP. Por lo tanto, la implementación de los puntos finales ZRTP seguirán dependiendo de la autenticación SAS durante un tiempo largo.

Incluso después de que haya una amplia disponibilidad de productos SIP que ofrezcan protección integrada, muchos usuarios se enfrentarán al hecho de que la ruta del proceso puede ser controlada por una serie de instrucciones que no esperan y la experiencia al usuario final será molesta. En esos casos, la autenticación SAS integrada de ZRTP seguirá siendo el único estándar para el usuario prudente. Eso, más las características de continuación.